Bounds for codes for a non-symmetric ternary channel

Ludo Tolhuizen, Philips Research Laboratories, Eindhoven, The Netherlands;
ludo.tolhuizen@philips.com

1   Introduction

In [1], a non-symmetric ternary communication channel inspired by 3-valued semiconductor memories was introduced, and error-correcting coding for this channel was studied. The authors of [1] showed the relevance of the minimum d_1-distance (defined below) of a ternary code for judging its error-correcting capabilities on this channel, gave a code construction, and derived a Hamming-like upper bound on the size of a code of given length and minimum d_1-distance. The work was extended in [2], where the authors obtained the channel capacity, and constructed optimal codes with a short length by techniques for finding cliques in graphs.

In the present paper, we give upper and lower bounds on the size of codes for the d_1-distance. We first introduce some notation.

We consider codes over the ternary alphabet $Q = \{-1, 0, 1\}$. For $\mathbf{x}, \mathbf{y} \in Q^n$, we define $d_1(\mathbf{x}, \mathbf{y})$ as

$$d_1(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} |x_i - y_i|.$$

For each $C \subseteq Q^n$, we denote the minimum d_1-distance between any two different words of C by $d_1(C)$. Furthermore, we define

$$T(n, d) = \max\{|C| \mid C \subset Q^n \text{ and } d_1(C) \geq d\}.$$

It is our aim to provide upper and lower bounds on $T(n, d)$. In the remainder of the paper, when we speak about "distance", we mean d_1-distance.

Unlike the Hamming distance, the d_1-distance is *not* translation-invariant. For example, the number of words at distance one from the all-zero word of length n equals $2n$, while the number of words of distance one from the all-one word of length n equals n. As a result, many bounds for codes in Hamming space [3] do not readily translate to codes for the d_1-distance. The Hamming bound from [1], for example, takes into account the largest balls and hence seems to be rather weak.

Some code constructions and bounds will use results for codes for the Hamming metric. The Hamming distance between two vectors $\mathbf{x}$ and $\mathbf{y}$ of equal length is denoted as $d_{\mathrm{H}}(\mathbf{x}, \mathbf{y})$. The minimum Hamming distance of a code C is denoted as $d_{\mathrm{H}}(C)$, and we define

$$A_q(n, d) = \max\{|C| \mid C \subset \{0, 1, \ldots q - 1\}^n \text{ and } d_{\mathrm{H}}(C) \geq d\}.$$

2   Bounds from code shortening and puncturing

Let $C \subseteq Q^n$ have minimum d_1-distance d. For $i \in Q$, we define

$$C_i = \{(x_1, x_2, \ldots x_{n-1}) \mid (x_1, x_2, \ldots, x_{n-1}, i) \in C\}.$$

We have the following easy proposition.

Proposition 1 *For each $i \in Q$, we have that $d_1(C_i) \geq d$, so $|C_i| \leq T(n-1, d)$;*
moreover, we have that $d_1(C_0 \cup C_1) \geq d - 1$, so $|C_0| + |C_1| \leq T(n-1, d-1)$;
and finally, $d_1(C_0 \cup C_1 \cup C_{-1}) \geq d - 2$.

Corollary 1 *The following inequalities are valid:*

$$T(n, d) \leq 3T(n-1, d) \tag{1}$$
$$T(n, d) \leq T(n-1, d) + T(n-1, d-1) \tag{2}$$
$$T(n, d) \leq T(n-1, d-2) \tag{3}$$

Proof. Let C have length n, minimum distance d, and size $T(n, d)$.
Inequality (1) follows from the fact that $T(n, d) = |C| = |C_{-1}| + |C_0| + |C_1| \leq 3T(n-1, d)$,
where the inequality follows from the first statement of Proposition 1.
Inequality (2) follows from the fact that $T(n, d) = |C| = |C_{-1}| + |C_0 \cup C_1| \leq T(n-1, d) + T(n-1, d-1)$, where the inequality follows from the two first statements of Proposition 1.
Inequality (3) is a direct consequence of the final statement in Propostion 1. $\quad\square$

Corollary 2 *For $n \geq 1$, we have that $T(n, 2) = (3^n + 1)/2$.*

Proof. Using Inequality (2) and induction on n, one readily finds that $T(n, 2) \leq \frac{1}{2}(3^n + 1)$.
The code consisting of all vectors of length n containing an even number of zeros, which is a special case of the construction in [1], has minimum distance two and $\frac{1}{2}(3^n + 1)$ words. $\quad\square$

3 Bounds and constructions based on codes for the Hamming distance

For any two ternary vectors $\mathbf{x}$ and $\mathbf{y}$ of equal length, we clearly have that $d_H(\mathbf{x}, \mathbf{y}) \leq d_1(\mathbf{x}, \mathbf{y}) \leq 2d_H(\mathbf{x}, \mathbf{y})$. As a consequence, for any ternary code C, we have that $d_H(C) \leq d_1(C) \leq 2d_H(C)$, and so

$$A_3(n, d) \leq T(n, d) \leq A_3\left(n, \left\lceil \frac{d}{2} \right\rceil\right). \tag{4}$$

Also, if $\mathbf{x}$ and $\mathbf{y}$ are two vectors over $\{-1, 1\}$, then $d_1(\mathbf{x}, \mathbf{y}) = 2d_H(\mathbf{x}, \mathbf{y})$, and so

$$T(n, d) \geq A_2\left(n, \left\lceil \frac{d}{2} \right\rceil\right). \tag{5}$$

Proposition 2 *We have that $\left(\frac{3}{4}\right)^n \cdot A_2(2n, d) \leq T(n, d) \leq A_2(2n, d)$.*

Proof. We define the mapping $\phi : Q \mapsto A := \{(0, 1), (0, 0), (1, 0)\}$ as

$$\phi(-1) = (0, 1), \phi(0) = (0, 0), \text{ and } \phi(1) = (1, 0),$$

and extend it to a mapping from Q^n to A^n by applying ϕ component-wise.
It is clear that for any $\mathbf{x}$ and $\mathbf{y}$ in Q^n, we have $d_1(\mathbf{x}, \mathbf{y}) = d_H(\phi(\mathbf{x}), \phi(\mathbf{y}))$. As a consequence,

for each $C \subseteq Q^n$, we have $d_1(C) = d_H(\phi(C))$, which implies the upper bound on $T(n, d)$. Conversely, let $C \subset \{0, 1\}^{2n}$ have minimum Hamming distance d. For each $\mathbf{c} \in C$, there are $|A|^n$ vectors $\mathbf{x}$ such that $\mathbf{x} + \mathbf{c} \in A^n$. Hence, for at least one of the 2^{2n} choices for $\mathbf{x}$, the size of $(\mathbf{x} + C) \cap A^n$ is at least $|C|A^n/2^{2n}$. As the minimum d_1-distance of $\phi^{-1}((\mathbf{x} + C) \cap A^n)$ equals $d_H((\mathbf{x} + C) \cap A^n) \geq d_H(\mathbf{x} + C) = d$, the lower bound follows. $\quad \square$

The elegant construction from [1] yields the following theorem.

Theorem 1 *Let C be a binary code with minimum Hamming distance d and A_w words of Hamming weight w ($w = 0, 1, \ldots, n$). Then*

$$T(n, d) \geq \sum_{w=0}^{n} A_w A_2 \left(w, \left\lceil \frac{d}{2} \right\rceil \right).$$

By averaging Theorem 1 over all cosets of C, we obtain the following corollary.

Corollary 3

$$T(n, d) \geq \frac{A_2(n, d)}{2^n} \sum_{w=0}^{n} \binom{n}{w} A_2 \left(w, \left\lceil \frac{d}{2} \right\rceil \right).$$

4   Plotkin bound

Theorem 2 below is an anlogon to the Plotkin bound for codes in Hamming space [3, Sec. 2.2], and is proved in Appendix A.

Theorem 2 *For $d > n$, we have that $T(n, d) \leq \frac{d}{d-n}$. A code attaining equality is a code over $\{-1, 1\}^n$ with minimum Hamming distance $d/2$ satisfying the binary Plotkin bound. Moreover, we have that*

$$T(d, d) \leq 2d + \frac{1}{2} + \sqrt{2d + \frac{1}{4}}.$$

5   Gilbert-Varshamov bounds

In this section, we derive lower bounds on $T(n, d)$ using the same arguments as for the Gilbert-Varshamov (GV) bound in Hamming space. The GV bound for codes with the Hamming metric guarantees the existence of a q-ary code of length n and minimum Hamming distance d with a cardinality at least $q^n/V_q(n, d - 1)$, where $V_q(n, r)$ denotes the cardinality of a ball of radius r in $\{0, 1, \ldots, q - 1\}$. The volume of a ball in the d_1-metric depends on its center. The generalized GV bound [4] guarantees the existence of a code of length n and minimum d_1-distance d with cardinality at least $3^n/\bar{V}(n, d - 1)$, where $\bar{V}(n, d - 1)$ is the *average* size of a ball of radius $d - 1$ in Q^n endowed with the d_1-metric. For computing this average size, we define $m(n, w)$ to be the number of ordered pairs of vectors in Q^n that have d_1-distance w. By induction on n, one readily obtains the following proposition.

Proposition 3 *We have that $\sum_{w=0}^{2n} m(n, w)z^w = (3 + 4z + 2z^2)^n$.*

By writing $(3 + 4z + 2z^2)^n = (2(1 + z)^2 + 1)^n$, expanding using the binomial theorem, and collecting terms of equal power, we obtain that $m(n, w) = \sum_{i=0}^{n} \binom{n}{i} 2^i \binom{2i}{w}$. The generalized GV bound [4] thus implies that

$$T(n, d) \geq \frac{3^{2n}}{\sum_{w=0}^{d-1} m(n, w)} = \frac{3^{2n}}{\sum_{w=0}^{d-1} \sum_{i=0}^{n} \binom{n}{i} 2^i \binom{2i}{w}}. \tag{6}$$

By applying the GV-argument to Q_w^n, the set of words in Q^n of Hamming weight w, we obtain that there exists a code in Q_w^n with minimum distance d and cardinality at least $|Q_w^n|/V(n, d-1, w)$, where $V(n, d-1, w)$ is the number of words in Q_w^n at distance at most $d - 1$ from a fixed word in Q_w^n. It is clear that $|Q_w^n| = \binom{n}{w} 2^w$. For obtaining $V(n, d-1, w)$, we use the following proposition.

Proposition 4 *For each $\mathbf{x} \in Q_w^n$ and each integer i, we have that*

$$|\{\mathbf{y} \in Q_w^n \mid d_1(\mathbf{x}, \mathbf{y}) = 2i + \epsilon\}| = \begin{cases} 0 & \text{if } \epsilon = 1, \\ \sum_j \binom{w}{j} \binom{w-j}{i-j} \binom{n-w}{j} 2^j & \text{if } \epsilon = 0. \end{cases}$$

Proof. Let $\mathbf{x} \in Q^n$ start with w ones and end in $n - w$ zeros. Let $\mathbf{y} \in Q_w^n$. We define j as the number of zeros in the w leftmost positions in $\mathbf{y}$, and $w - i$ as the number of ones in the leftmost positions of $\mathbf{y}$. Then $(i - j)$ of the w leftmost entries of $\mathbf{y}$ equal -1, and, as $\mathbf{y}$ has weight w, j entries of the righmost values of $\mathbf{y}$ are non-zero. We conclude that the number of vectors $\mathbf{y}$ satisfying the above constraint equals

$$\binom{w}{j} \binom{w-j}{i-j} \binom{n-w}{j} 2^j,$$

while $d_1(\mathbf{x}, \mathbf{y}) = j + 2(i - j) + j = 2i$. $\quad\square$

We conclude that the following theorem holds.

Theorem 3 *For each $w, 1 \leq w \leq n$, we have that*

$$T(n, d) \geq \frac{\binom{n}{w} 2^w}{\sum_{i=0}^{(d-1)/2} \sum_{j=0}^{\min(i, n-w, w)} \binom{w}{j} \binom{n-w}{j} \binom{w-j}{i-j} 2^j}.$$

6 Asymptotics of the bounds

In this section, we derive the asymptotic versions of the obtained bounds. For $0 < \delta < 2$, we define

$$\tau(\delta) = \lim_{n \to \infty} \sup \frac{1}{n} \log_3(T(n, \lceil \delta n \rceil)).$$

For $0 < \delta < 1$, we define

$$\alpha_q(\delta) = \lim_{n \to \infty} \sup \frac{1}{n} \log_q(A_q(n, \lceil \delta n \rceil)).$$

We will use the asymptotic GV bound: for $0 \leq \delta \leq 1 - \frac{1}{q}$, we have

$$\alpha_q(\delta) \geq 1 - h_q(\delta), \tag{7}$$

where h_q is the q-ary entropy function, defined as

$$h_q(x) = -x \log_q(x) - (1 - x) \log_q(1 - x) + x \log_q(q - 1). \qquad (8)$$

The following inequalities are readily obtained from (4), (5), and Proposition 2

$$\alpha_3(\delta) \leq \tau(\delta) \leq \alpha_3\left(\frac{\delta}{2}\right) \qquad (9)$$

$$\tau(\delta) \geq \log_3(2)\alpha_2\left(\frac{\delta}{2}\right) \qquad (10)$$

$$\tau(\delta) \leq 2\log_3(2)\alpha_2\left(\frac{\delta}{2}\right) \qquad (11)$$

$$\tau(\delta) \geq \log_3\left(\frac{3}{4}\right) + 2\log_3(2)\alpha_2\left(\frac{\delta}{2}\right) \qquad (12)$$

As $\alpha_2(\delta) > 0$ if and only if $\delta < \frac{1}{2}$, we derive from (10) and (11) that $\tau(\delta) > 0$ if and only if $\delta < 1$.

The asymptotic version of Corollary 3 is

$$\tau(\delta) \geq \log_3(2)\left(-1 + \alpha_2(\delta) + \sup_{\max(\delta,1/2)<\omega<1} \{h_2(\omega) + \omega\alpha_2(\delta/(2\omega))\}\right). \qquad (13)$$

Using the asymptotic binary GV bound (7) we find that (13) implies that

$$\tau(\delta) \geq \log_3(2)\left(-1 + \alpha_2(\delta) + \sup_{\max(\delta,1/2)<\omega<1} \{h_2(\omega) + \omega\left(1 - h_2(\delta/(2\omega))\right)\}\right). \qquad (14)$$

If $\delta \leq 1/2$, the supremum in (14) is attained for $\omega = \frac{1}{6}(2 + \delta + \sqrt{4 - 8\delta + \delta^2})$.

The asymptotic form of the generalized GV bound (6) is

$$\tau(\delta) \geq 2 - \log_3(2) \sup_{\substack{0<\omega<1 \\ 0<\beta<\min(\delta,2\omega)}} \left\{h_2(\omega) + 2\omega h_2\left(\frac{\beta}{2\omega}\right) + \omega\right\}. \qquad (15)$$

If $\delta \geq 8/9$, the supremum in (15) is attained for $\omega = \beta = 8/9$, and we obtain the trivial inequality $\tau(\delta) \geq 0$.

Otherwise, if $\delta < 8/9$, we obtain, by setting the partial deriviatives with respect to β and ω equal to zero, that the supremum in (15) is attained for $\beta = \delta$ and $\omega = (2 + \delta + \sqrt{2(-\delta^2 + 2\delta + 2)})/6$.

The asymptotic version of Theorem 3, the GV bound for constant-weight ternary codes, is the following. For every $\omega, 0 < \omega < 1$, we have that

$$\tau(\delta) \geq \log_3(2)[h_2(\omega) + \omega - \sup_{\substack{0<\beta<\min(\delta/2,\omega) \\ 0<\gamma<\min(\beta,\omega,1-\omega)}} \left\{\omega h_2\left(\frac{\gamma}{\omega}\right) + (1 - \omega)h_2\left(\frac{\gamma}{1 - \omega}\right)\right.$$
$$\left. + (\omega - \gamma)h_2\left(\frac{\beta - \gamma}{\omega - \gamma}\right) + \gamma\right\}] . \qquad (16)$$

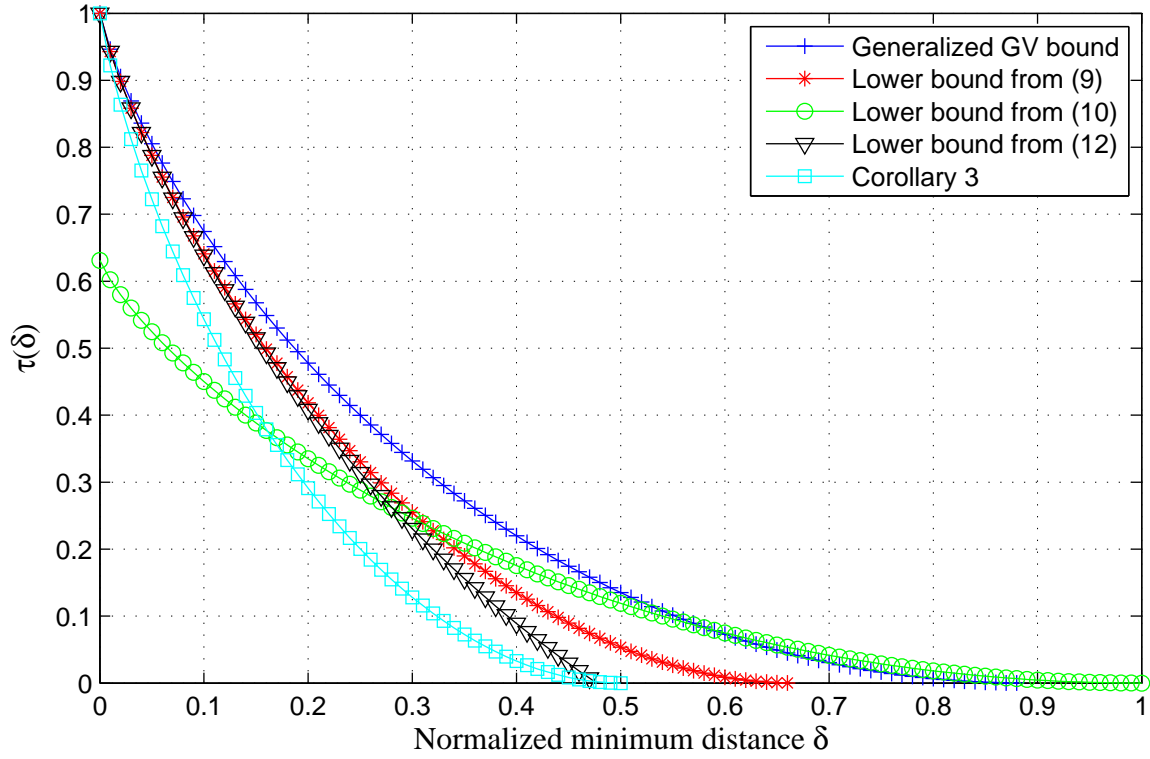Figure 1: Lower bounds on $\tau(\delta)$.

If $\delta \geq \omega(2 - \omega)$, the supremum in (16) is attained for $\beta = \frac{1}{2}\omega(2 - \omega)$ and $\gamma = \omega(1 - \omega)$, and we obtain the trivial inequality $\tau(\delta) \geq 0$.

If $\delta < \omega(2 - \omega)$, the supremum in (16) is attained for $\beta = \delta/2$ and $\gamma = 1 - \omega + \delta/2 - \sqrt{(1 - \omega)^2 + \frac{1}{4}\delta^2}$.

Next, for fixed δ, we optimize (16) over ω, using the values for β and γ obtained before. As shown in Appendix B, the optimzing value for ω equals $\omega = \frac{1}{3}(1 + \delta + \sqrt{\delta^2 - \delta + 1})$.

Note that for $\delta = 0$, the optimizing ω, as expected, equals $\frac{2}{3}$, while for $\delta = 1$, the optimal value is $\omega = 1$, i.e., for large δ, binary codes are good.

7 Comparison of asymptotic lower bounds

In Figure 1, we plot the various asymptotic lower bounds on $\tau(\delta)$. We have used the GV bound (7) to lower bound $\alpha_q(\delta)$. It is interesting to see that for large δ, the bound from (10), obtained using the GV bound for binary codes, performs better than the generalized GV bound for ternary codes with the d_1-distance from (15). This shows some similarity to the result from [2] that states that for large cross-over probabilities, channel capacity is achieved by a binary code.

In Figure 2, we plot the generalized GV bound and the bound from (16) optimized over ω, i.e., for each value of δ the expression from (16) is optimized over ω. For comparison purposes, we have also plotted the bound from (16) for $\omega = 2/3$. Note that the asymptotic GV bound for constant-weight codes (16) slighly improves the generalized GV bound when we optimize over ω.
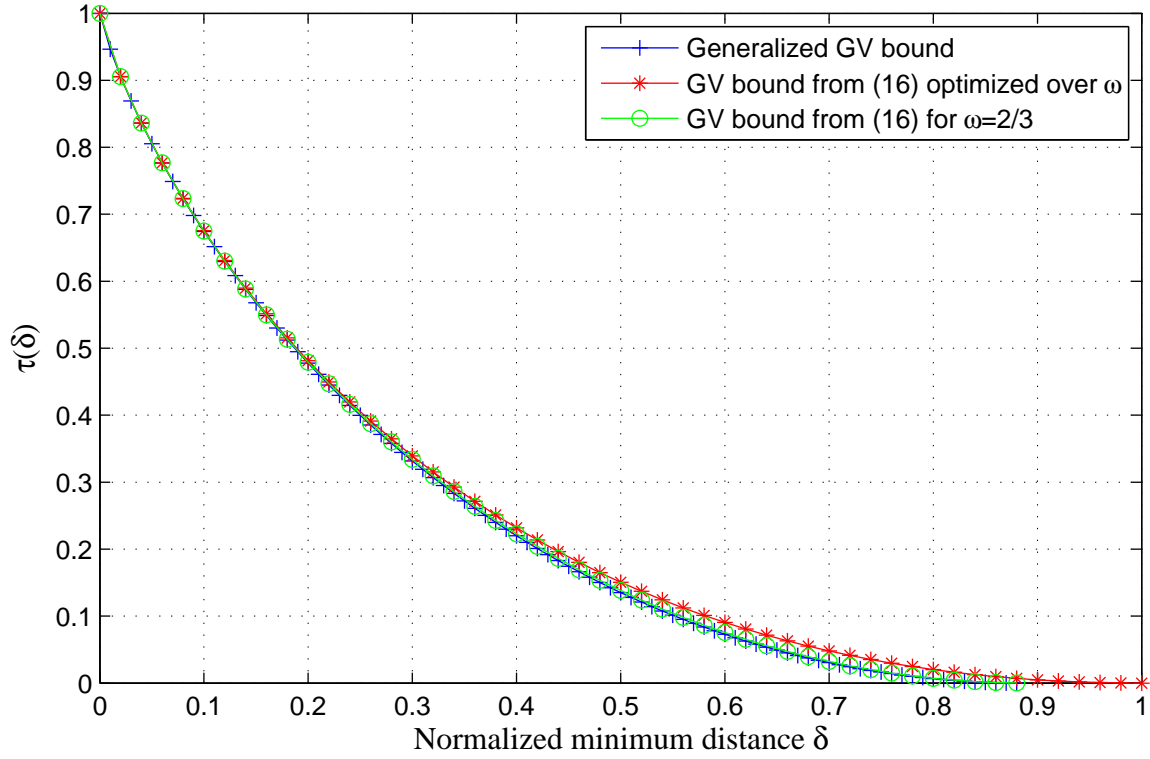
Figure 2: Lower bounds on $\tau(\delta)$.

Acknowledgement

Appendix A: Proof of Theorem 2

Let C be a code of length n, minimum distance d, and M words. For $1 \leq i \leq n$ and $j \in Q$, we define $m_j(i) = |\{\mathbf{c} \in C \mid c_i = j\}|$. We define S as $S = \sum_{\mathbf{x} \in C} \sum_{\mathbf{y} \in C} d_1(\mathbf{x}, \mathbf{y})$. We obviously have that $S \geq M(M-1)d$. On the other hand,

$$S = \sum_{i=1}^{n} m_0(i)[m_1(i) + m_{-1}(i)] + m_1(i)[m_0(i) + 2m_{-1}(i)] + m_{-1}(i)[m_0(i) + 2m_1(i)]$$

$$= \sum_{i=1}^{n} 2m_0(i)[m_1(i) + m_{-1}(i)] + 4m_1(i)m_{-1}(i).$$

For each $i \in \{1, \ldots, n\}$, we have that

$$4m_1(i)m_{-1}(i) = (m_1(i) + m_{-1}(i))^2 - (m_1(i) - m_{-1}(i))^2 \leq (m_1(i) + m_{-1}(i))^2.$$

Moreover, as $m_1(i) + m_{-1}(i) = M - m_0(i)$, we obtain that

$$S \le \sum_{i=1}^{n} 2m_0(i)(M - m_0(i)) + (M - m_0(i))^2 = \sum_{i=1}^{n}(M - m_0(i))(M + m_0(i))$$

$$= nM^2 - \sum_{i=1}^{n} m_0^2(i).$$

As a consequence, we have that

$$M(M - 1)d \le S \le nM^2 - \sum_{i=1}^{n} m_0^2(i). \tag{17}$$

Inequality (17) clearly implies that $M(M - 1)d \le nM^2$, and so, if $d > n$, we have that $M \le d/(d - n)$. If equality holds, we must have that $\sum_{i=1}^{n} m_0^2(i) = 0$, so $C \subset \{-1, 1\}^n$. If $d = n$, (17) says that $\sum_{i=1}^{n} m_0^2(i) \le Mn$. Hence, for some i, we have that $m_0^2(i) \le M$. By shortening in position i,w e obtain three codes of length $n - 1$ and minimum distance d, and (using the same notation as in Section 2), we find that

$$M = |C_0| + |C_{-1}| + |C_1| \le \sqrt{M} + 2T(d-1, d) \le \sqrt{M} + 2d, \text{ whence } (\sqrt{M} - \frac{1}{2})^2 \le 2d + \frac{1}{4}. \quad \square$$

Appendix B: Optimizing (16) over ω

Setting the partial derivative of the right hand side of (16) with respect to ω to zero, with $\beta = \delta/2$ and $\gamma = 1 - \omega + \delta/2 - \sqrt{(1 - \omega)^2 + \frac{1}{4}\delta^2}$, results in the following equation:

$$3\omega^4 - 2(4 + \delta)\omega^3 + 4(1 + 2\delta)\omega^2 - 2\delta(2 + \delta)\omega + \delta^2 = 0. \tag{18}$$

The polynomial in (18) factors as $(\omega^2 - 2\omega + \delta)(3\omega^2 - 2(\delta + 1)\omega + \delta)$, so that we find the four roots for the polynomial, viz.

$$1 - \sqrt{1 - \delta}, \ 1 + \sqrt{1 - \delta}, \ \frac{1}{3}(1 + \delta - \sqrt{\delta^2 - \delta + 1}), \text{ and } \frac{1}{3}(1 + \delta + \sqrt{\delta^2 - \delta + 1}).$$

Note that in order to find a non-zero solution in (16), it is required that $\delta > \omega(2 - \omega)$, and $\frac{1}{3}(1 + \delta + \sqrt{\delta^2 - \delta + 1})$ is the only root satisfying this requirement.

References

[1] N. Bitouzé and A. Graell i Amat, "Coding for a non-symmetric ternary channel", in *Proc. Inform. Th. and Appl. Workshop (ITA 2009)*, Feb. 2009, pp. 113-118.

[2] N. Bitouzé, A. Graell i Amat, and E. Rosnes, "Error correcting coding for a non-symmetric ternary channel," arXiv:0911.1072, Nov. 5, 2009.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, 1977.

[4] L. M. G. M. Tolhuizen, "The generalized Gilbert-Varshamov bound is implied by Turán's theorem," *IEEE Trans. Inform. Th.*, vol. 43, no. 5, Sept. 1997, pp. 1605–1606.